Chapter 4

Ethical and Social Issues in Information Systems

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

1. Analyze the relationships among ethical, social, and political issues that are raised by information systems.
2. Identify the main moral dimensions of an information society and specific principles for conduct that can be used to guide ethical decisions.
3. Evaluate the impact of contemporary information systems and the Internet on the protection of individual privacy and intellectual property.
4. Assess how information systems have affected everyday life.

Interactive Sessions:

Data for Sale

The Internet: Friend or Foe to Children?

CHAPTER OUTLINE

DOES LOCATION TRACKING THREATEN PRIVACY?

For many years, parents of District of Columbia public school children complained about buses running late or not showing up. A federal court appointed an independent transportation administrator and enlisted Satellite Security Systems, or S3, to track the movements of the district's buses. S3 provides satellite tracking services to clients such as the District of Columbia, Fairfax County, state and federal government agencies, police departments, and private companies.

These services equip each vehicle or person they are monitoring with a tracking device using global positioning system (GPS) technology. GPS is a navigation system operated by the U.S. Department of Defense based on satellites that continually broadcast their position, time, and date. GPS receivers on the ground, which can be attached to vehicles, cell phones, or other equipment, use information from the satellite signals to calculate their own locations. Cell phones are now equipped with GPS.

The D.C. public school system is spending $6 million on its GPS tracking system. It is equipping buses with GPS locators and special-needs children riding those buses with ID cards that log when they get on and off their buses. Parents receive secret codes that enable them to use the Internet to track their children. S3's monitoring center picks up GPS information from the tracking devices and monitors the locations of the buses on video screens. Most of the monitoring is automated, and the S3 staff intervenes primarily in emergencies. S3 maintains each day's tracking data for long periods, and clients can access historical tracking data if they wish.

S3 provides detailed information to the D.C. public schools: each bus's route throughout the day, when the bus stops, when the doors open and close, the speed, and when the ignition is turned on and off. The S3 system includes a database with information on the bus passengers—each child's name, address, disabilities, allergies, contact information, and when their school days begin and end.

David Gilmore, the court-appointed transportation administrator for the D.C. public schools has seen improvement in bus driver performance. Reports of bus drivers making detours to banks or to take long lunches are diminishing.

Parents are also pleased. "I like that the system lets you watch them, because you never know what's going on in the bus," says Deneen Prior, whose three children ride D.C. public school buses. However, she also worries about the location tracking data being misused. "I don't want anybody watching them that's not supposed to be watching them," she notes.

Others feel the same way. Location tracking has benefits, but it also opens the door to potential invasion of privacy. Many people may not like having their physical move-

ments tracked so closely. Location information might help direct a tow truck to a broken-down car, but it could also be used to find out where the driver went during the lunch hour.

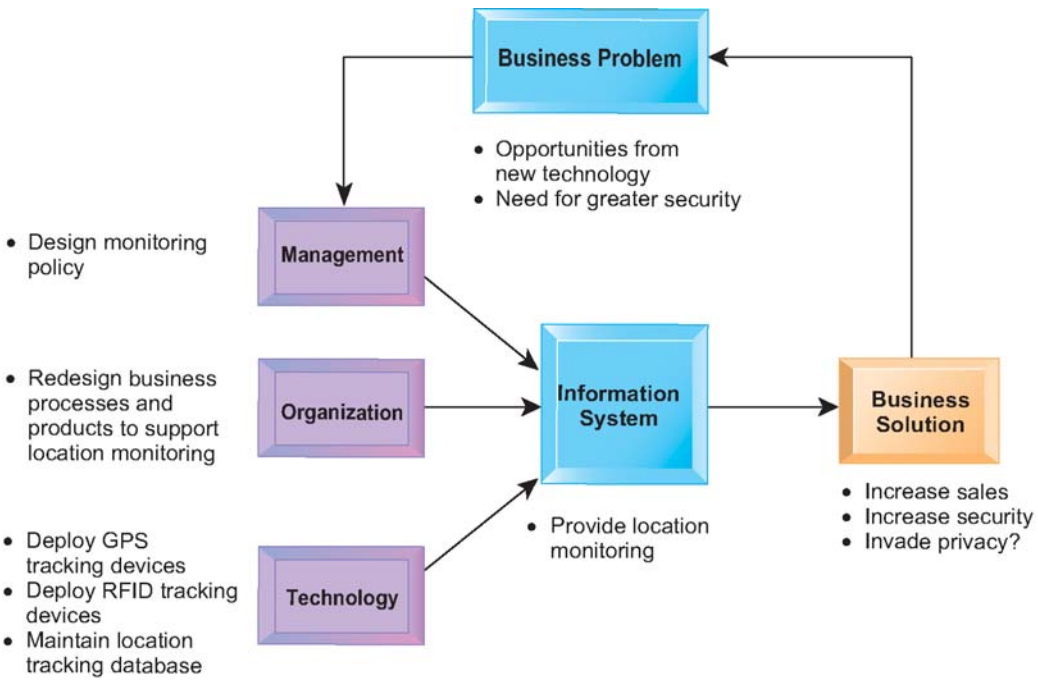
For similar reasons, privacy advocacy groups have opposed the use of radio-frequency identification (RFID) tags in consumer items. RFID tags are small silicon chips equipped with tiny antennas that enable them to communicate with RFID readers and track the location of items as they move. When placed on individual products, they allow companies to tell exactly when a product leaves a store or learn more about the actions of consumers buying the products.

Designer Lauren Scott had planned to add radio frequency tags to the childrens' clothing she designed to help parents keep track of their children. An RFID tag sewn into a child's clothing could store vital medical information or track the wearer's location to prevent children from being abducted or wandering away. As a result of the controversy surrounding RFID, however, several of Scott's major customers asked that the tags not be sewn directly into the clothing.

Sources: Mel Duvall, "At the Seams of RFID," *Baseline*, April 2006; Ariana Eunjung Cha, "To Protect and Intrude," *The Washington Post*, January 15, 2005; and Christopher Lindquist, "Watch Carefully," *CIO Magazine*, May 15, 2005.

The use of location tracking systems described in the chapter-opening case shows that technology can be a double-edged sword. It can be the source of many benefits, and it can also create new opportunities for breaking the law or taking benefits away from others.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. The D.C. public school system faced a real problem in trying to make sure its drivers were transporting children safely and promptly to school. Location tracking technology provided a solution, but it also introduced the possibility that information about the people or vehicles S3



tracked could be used for the wrong purpose. Location tracking technology had a similar impact for designer Lauren Scott's children's clothing business.

This solution created what we call an "ethical dilemma," pitting the legitimate need to know what drivers of school buses were doing with the fear that such information could be used to threaten individual privacy. Another ethical dilemma might occur if you were implementing a new information system that reduced labor costs and eliminated employees' jobs. You need to be aware of the negative impacts of information systems and you need to balance the negative consequences with the positive ones.

HEADS UP

Information systems raise new and often-perplexing ethical problems. This is more true today than ever because of the challenges posed by the Internet and electronic commerce to the protection of privacy and intellectual property. Other ethical issues raised by widespread use of information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protect the safety of individuals and society, and preserving values and institutions considered essential to the quality of life in an information society. Whether you run your own business or work in a large company, you'll be confronting these issues, and you'll need to know how to deal with them.

- If your career is in finance and accounting, you will need to ensure that the information systems you work with are protected from computer fraud and abuse.
- If your career is in human resources, you will be involved in developing and enforcing a corporate ethics policy and in providing special training to sensitize managers and employees to the new ethical issues surrounding information systems.
- If your career is in information systems, you will need to make management aware of the ethical implications of the technologies used by the firm and help management establish code of ethics for information systems.
- If your career is in manufacturing, production, or operations management, you will need to deal with data quality and software problems that could interrupt the smooth and accurate flow of information among disparate manufacturing and production systems and among supply chain partners.
- If your career is in sales and marketing, you will need to balance systems that gather and analyze customer data with the need for protecting consumer privacy.

4.1 Understanding Ethical and Social Issues Related to Systems

In the past five years we have witnessed, arguably, one of the most ethically challenging periods for U.S. and global business. Table 4-1 provides a small sample of recent cases demonstrating failed ethical judgment by senior and middle managers. These lapses in management ethical and business judgment occurred across a broad spectrum of industries.

In today's new legal environment, managers who violate the law and are convicted will most likely spend time in prison. U.S. Federal Sentencing

TABLE 4-1 EXAMPLES OF FAILED ETHICAL JUDGMENT BY MANAGERS

Enron	Top three executives convicted for misstating earnings using illegal accounting schemes and making false representations to shareholders. Bankruptcy declared in 2001.
WorldCom	Second-largest U.S. telecommunications firm. Chief executive convicted for improperly inflating revenue by billions using illegal accounting methods. Bankruptcy declared in July 2002 with $41 billion in debts.
Merrill Lynch	Indicted for assisting Enron in the creation of financial vehicles that had no business purpose, enabling Enron to misstate its earnings.
Parmalat	Italy's eighth-largest industrial group indicted for misstating more than $5 billion in revenues, earnings, and assets over several years; senior executives indicted for embezzlement.
Bristol-Myers Squibb	Pharmaceutical firm agreed to pay a fine of $150 million for misstating its revenues by $1.5 billion and inflating its stock value.
Brocade Communications Systems, Inc.	Gregory Reyes, the CEO of Brocade Communications Systems Inc. until January 2005, indicted in criminal and civil cases in 2006 of backdating options and concealing millions of dollars of compensation expenses from shareholders. Nearly 100 other Silicon Valley tech firms are under investigation for similar practices.
KPMG LLP, Ernst & Young, and PricewaterhouseCoopers	Senior tax accountants of three of the leading "Big Four" public accounting firms are indicted by the Justice Department over the selling of abusive tax shelters to wealthy individuals in the period 2000-2005. This case is frequently referred to as the "largest tax fraud case in history."

Guidelines adopted in 1987 mandate that federal judges impose stiff sentences on business executives based on the monetary value of the crime, the presence of a conspiracy to prevent discovery of the crime, the use of structured financial transactions to hide the crime, and failure to cooperate with prosecutors (U.S. Sentencing Commission, 2004).

Although in the past, business firms would often pay for the legal defense of their employees enmeshed in civil charges and criminal investigations, now firms are encouraged to cooperate with prosecutors to reduce charges against the entire firm for obstructing investigations. These developments mean that, more than ever, as a manager or an employee, you will have to decide for yourself what constitutes proper legal and ethical conduct.

Although these major instances of failed ethical and legal judgment were not masterminded by information systems departments, information systems were instrumental in many of these frauds. In many cases, the perpetrators of these crimes artfully used financial reporting information systems to bury their decisions from public scrutiny in the vain hope they would never be caught. We deal with the issue of control in information systems in Chapter 8. In this chapter we talk about the ethical dimensions of these and other actions based on the use of information systems.

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technologies, such as steam engines, electricity, the telephone, and the radio, information technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others.

Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute

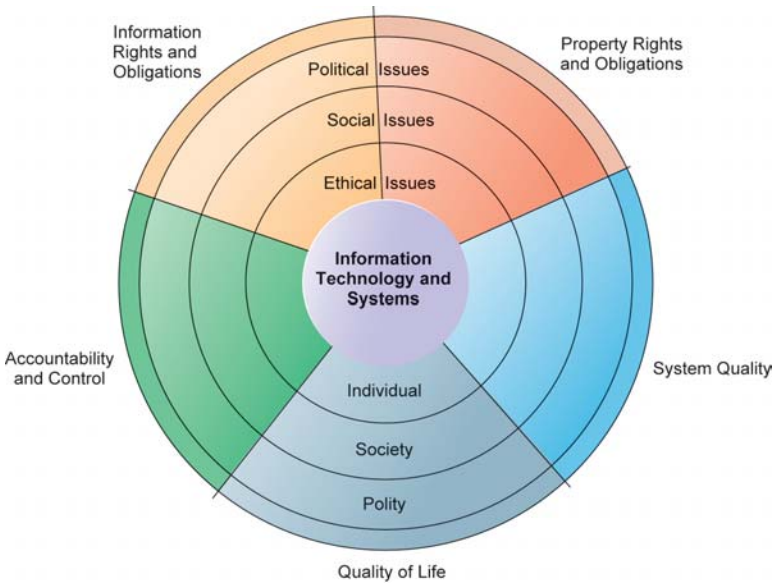
information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property. Insiders with special knowledge can "fool" information systems by submitting phony records, and diverting cash, on a scale unimaginable in the pre-computer era.

Other pressing ethical issues raised by information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protects the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, "What is the ethical and socially responsible course of action?"

A MODEL FOR THINKING ABOUT ETHICAL, SOCIAL, AND POLITICAL ISSUES

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is given in Figure 4-1. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behavior, and these are supported by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. But imagine instead of a rock that the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. What happens? Ripples, of course.

FIGURE 4-1 **THE RELATIONSHIP BETWEEN ETHICAL, SOCIAL, AND POLITICAL ISSUES IN AN INFORMATION SOCIETY**



The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

Suddenly individual actors are confronted with new situations often not covered by the old rules. Social institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, social responsibility, politically correct attitudes, or approved rules. Political institutions also require time before developing new laws and often require the demonstration of real harm before they act. In the meantime, you may have to act. You may be forced to act in a legal gray area.

We can use this model to illustrate the dynamics that connect ethical, social, and political issues. This model is also useful for identifying the main moral dimensions of the information society, which cut across various levels of action—individual, social, and political.

FIVE MORAL DIMENSIONS OF THE INFORMATION AGE

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

Information rights and obligations. What **information rights** do individuals and organizations possess with respect to themselves? What can they protect? What obligations do individuals and organizations have concerning this information?

Property rights and obligations. How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?

Accountability and control. Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?

System quality. What standards of data and system quality should we demand to protect individual rights and the safety of society?

Quality of life. What values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

We explore these moral dimensions in detail in Section 4.3.

KEY TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

Ethical issues long preceded information technology. Nevertheless, information technology has heightened ethical concerns, taxed existing social arrangements, and made some laws obsolete or severely crippled. Information technologies and systems have also created new opportunities for criminal behavior and mischief. There are four key technological trends responsible for these ethical stresses and they are summarized in Table 4-2.

TABLE 4-2 TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

TREND	IMPACT
Computing power doubles every 18 months	More organizations depend on computer systems for critical operations.
Data storage costs rapidly declining	Organizations can easily maintain detailed databases on individuals.
Data analysis advances	Companies can analyze vast quantities of data gathered on individuals to develop detailed profiles of individual behavior.
Networking advances and the Internet	Copying data from one location to another and accessing personal data from remote locations are much easier.

The doubling of computing power every 18 months has made it possible for most organizations to use information systems for their core production processes. As a result, our dependence on systems and our vulnerability to system errors and poor data quality have increased. The very same information systems that lead to high levels of productivity also create opportunities for abuse. Social rules and laws have not yet adjusted to this dependence. Standards for ensuring the accuracy and reliability of information systems (see Chapter 8) are not universally accepted or enforced.

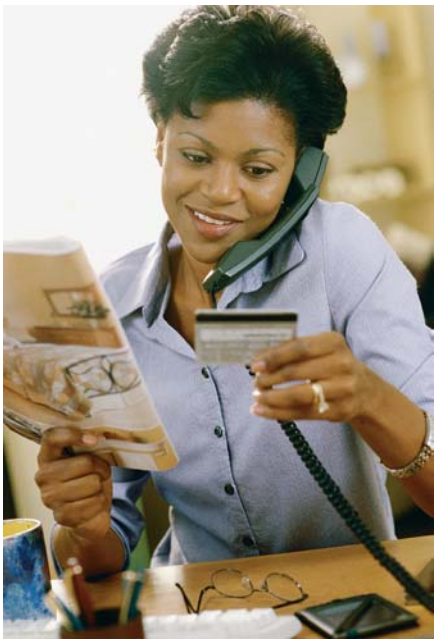
Advances in data storage techniques and rapidly declining storage costs have been responsible for the multiplying databases on individuals—employees, customers, and potential customers—maintained by private and public organizations. These advances in data storage have made the routine violation of individual privacy both cheap and effective. Already, massive data storage systems are cheap enough for regional and even local retailing firms to use in identifying customers. For instance, the major search firms like Google, America Online (AOL), MSN, and Yahoo! maintain detailed search histories on the more than 75 million Americans who use Internet search engines everyday and who generate more than 200 million searches each day. These huge collections of "consumer intentions" become the natural targets of private firms looking for market advantage, government agencies, and private investigators.

Advances in data analysis techniques for large pools of data are another technological trend that heightens ethical concerns because companies and government agencies are able to find out much detailed personal information about individuals. With contemporary data management tools (see Chapter 6), companies can assemble and combine the myriad pieces of information about you stored on computers much more easily than in the past.

Think of all the ways you generate computer information about yourself—credit card purchases; telephone calls; magazine subscriptions; video rentals; mail-order purchases; banking records; local, state, and federal government records (including court and police records); and visits to Web sites to read Web materials, use search engines, and write blogs (see Chapter 10). Put together and mined properly, this information could reveal not only your credit information but also your driving habits, your tastes, your associations, intended purchases, political views, and interests. What you thought was private, in fact, can quickly become public.

Companies with products to sell purchase relevant information from these sources to help them more finely target their marketing campaigns. Chapters 3 and 6 describe how companies can analyze large pools of data from multiple sources to rapidly identify buying patterns of customers and suggest individual responses. The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals is called **profiling**.

For example, hundreds of Web sites allow DoubleClick (www.doubleclick.net), an Internet advertising broker, to track the activities of their visitors in exchange for revenue from advertisements based on visitor information DoubleClick gathers. DoubleClick uses this information to create a profile of each online visitor, adding more detail to the profile as the visitor accesses an associated DoubleClick site. Over time, DoubleClick can create a detailed dossier of a person's spending and computing habits on the Web that can be sold to companies to help them target their Web ads more precisely.



Credit card purchases can make personal information available to market researchers, telemarketers, and direct-mail companies. Advances in information technology facilitate the invasion of privacy.

ChoicePoint, described in the Interactive Session on Management, gathers data from police, criminal, and motor vehicle records; credit and employment histories; current and previous addresses; professional licenses; and insurance claims to assemble and maintain electronic dossiers on almost every adult in the United Sates. The company sells this personal information to businesses and government agencies. Demand for personal data is so enormous that data broker businesses such as ChoicePoint are booming.

A new data analysis technology called **nonobvious relationship awareness (NORA)** has given both the government and the private sector even more powerful profiling capabilities. NORA can take information about people from many disparate sources, such as employment applications, telephone records, customer listings, and "wanted" lists, and correlate relationships to find obscure hidden connections that might help identify criminals or terrorists (see Figure 4-2). For instance, an applicant for a government security job might have received phone calls from a person wanted by the police. This diad (grouping of two) might also share the same religion, attend the same church, and be part of a small group with frequent telephone contacts.

NORA technology scans data and extracts information as the data are being generated so that it could, for example, instantly discover a man at an airline ticket counter who shares a phone number with a known terrorist before that person boards an airplane. The technology is considered a valuable tool for homeland security but does have privacy implications because it can provide such a detailed picture of the activities and associations of a single individual.

Finally, advances in networking, including the Internet, promise to reduce greatly the costs of moving and accessing large quantities of data and open the possibility of mining large pools of data remotely using small desktop machines, permitting an invasion of privacy on a scale and with a precision heretofore unimaginable. If computing and networking technologies continue to advance at the same pace as in the past, by 2023, large organizations will be

INTERACTIVE SESSION: MANAGEMENT

DATA FOR SALE

Want a list of 3,877 charity donors in Detroit? You can buy it from USAData for $465.24. Through USAData's Web site, which is linked to large databases maintained by Acxiom and Dun & Bradstreet, anyone with a credit card can buy marketing lists of consumers broken down by location, demographics, and interests. The College Board sells data on graduating high school seniors to 1,700 colleges and universities for 28 cents per student. These businesses are entirely legal. Also selling data are businesses that obtain credit card and cell phone records illegally and sell to private investigators and law enforcement. The buying and selling of personal data has become a multibillion dollar business that's growing by leaps and bounds.

Unlike banks or companies selling credit reports, these private data brokers are largely unregulated. There has been little or no federal or state oversight of how they collect, maintain, and sell their data. But they have been allowed to flourish because there is such a huge market for personal information and they provide useful services for insurance companies, banks, employers, and federal, state, and local government agencies.

For example, the Internal Revenue Service and departments of Homeland Security, Justice, and State paid data brokers $30 million in 2005 for data used in law enforcement and counterterrorism. The Internal Revenue Service signed a five-year $200 milllion deal to access ChoicePoint's databases to locate assets of delinquent taxpayers. After the September 11, 2001 terrorist attacks, ChoicePoint helped the U.S. government screen candidates for the new federally controlled airport security workforce.

ChoicePoint is one of the largest data brokers, with more than 5,000 employees serving businesses of all sizes as well as federal, state, and local governments. In 2004, ChoicePoint performed more than seven million background checks. It processes thousands of credit card transactions every second.

ChoicePoint builds its vast repository of personal data through an extensive network of contractors who gather bits of information from public filings, financial-services firms, phone directories, and loan application forms. The contractors use police departments, school districts, the department of motor vehicles, and local courts to fill their caches. All of the information is public and legal.

ChoicePoint possesses 19 billion records containing personal information on the vast majority of American adult consumers. According to Daniel J. Solove, associate professor of law at George Washington University, the company has collected information on nearly every adult American and "these are dossiers that J. Edgar Hoover would be envious of."

The downside to the massive databases maintained by ChoicePoint and other data brokers is the threat they pose to personal privacy and social well being. The quality of the data they maintain can be unreliable, causing people to lose their jobs and their savings. In one case, Boston Market fired an employee after receiving a background check from ChoicePoint that showed felony convictions. However, the report had been wrong. In another, a retired GE assembly-line worker was charged a higher insurance premium because another person's driving record, with multiple accidents, had been added to his ChoicePoint file.

ChoicePoint came under fire in early 2005 for selling information on 145,000 customers to criminals posing as legitimate businesses. The criminals then used the identities of some of individuals on whom ChoicePoint maintained data to open fraudulent credit card accounts.

Since then ChoicePoint curtailed the sale of products that contain sensitive data, such as social security and driver's license ID numbers, and limited access by small businesses, including private investigators, collection agencies, and non-bank financial institutions. ChoicePoint also implemented more stringent processes to verify customer authenticity.

Marc Rotenberg of the Electronic Privacy Information Center in Washington, D.C., believes that the ChoicePoint case is a clear demonstration that self-regulation does not work in the information business and that more comprehensive laws are needed. California, 22 other states, and New York City have passed laws requiring companies to inform customers when their personal data files have been compromised. More than a dozen data security bills were introduced in Congress in 2006 and some type of federal data security and privacy legislation will

likely result. Privacy advocates are hoping for a broad federal law with a uniform set of standards for privacy protection practices.

Sources: Rick Whiting, "Who's Buying and Selling Your Data? Everybody," *Information Week*, July 10, 2006; Christopher Wolf, "Dazed and Confused: Data Law Disarray," *Business Week*, June 8, 2006; Evan Perez and Rick Brooks, "For Big Vendor of Personal Data, A Theft Lays Bare the Downside," *The Wall Street Journal*, May 3, 2005; and "ChoicePoint Toughens Data Security," *CNN/Money*, July 5, 2005.

CASE STUDY QUESTIONS

1. Do data brokers pose an ethical dilemma? Explain your answer.
2. What are the problems caused by the proliferation of data brokers? What management, organization, and technology factors are responsible for these problems?
3. How effective are existing solutions to these problems?
4. Should the U.S. federal government regulate private data brokers? Why or why not? What are the advantages and disadvantages?

MIS IN ACTION

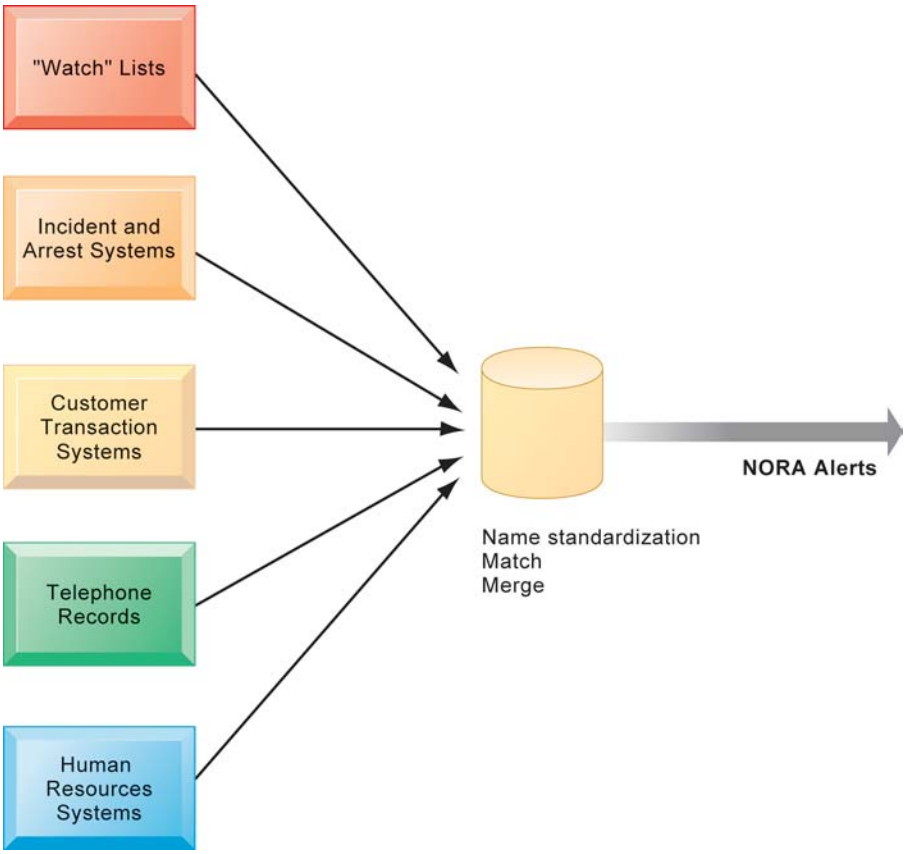
Explore the Web site of USAData (usadata.com). Click on Consumer Mailing Lists/Sales Leads to start the process of ordering a consumer mailing list online but do not use your credit card to pay for the list. Answer the following questions:

1. What kind of data does this company provide? How does it obtain the data?
2. Who uses the data sold by USAData? Are there any restrictions on who can use the data?
3. What kind of information can you obtain by ordering a mailing list online? How detailed is this information? How easy is it to purchase this information? Can someone use this online capability to find out how much money you make?
4. Does the capability of USAData raise privacy issues? What are they?
5. If your name and other personal information were in this database, what limitations on access would you want in order to preserve your privacy? Consider the following data users: (a) government agencies, (b) your employer, (c) private business firms, (d) other individuals.

able to devote the equivalent of a contemporary desktop personal computer to monitoring each of the 350 million individuals who will then be living in the United States (Farmer and Mann, 2003).

The development of global digital communication networks widely available to individuals and businesses poses many ethical and social concerns. Who will account for the flow of information over these networks? Will you be able to trace information collected about you? What will these networks do to the traditional relationships between family, work, and leisure? How will traditional job designs be altered when millions of "employees" become subcontractors using mobile offices for which they themselves must pay? In the next section we consider some ethical principles and analytical techniques for dealing with these kinds of ethical and social concerns.

FIGURE 4-2 NONOBVIOUS RELATIONSHIP AWARENESS (NORA)



NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

4.2 Ethics in an Information Society

Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

BASIC CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. **Responsibility** is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make.

Accountability is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action. Liability extends the concept of responsibility further to the area of laws.

Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. **Due process** is a related feature of law-governed societies and is a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

These basic concepts form the underpinning of an ethical analysis of information systems and those who manage them. First, information technologies are filtered through social institutions, organizations, and individuals. Systems do not have impacts by themselves. Whatever information system impacts exist are products of institutional, organizational, and individual actions and behaviors. Second, responsibility for the consequences of technology falls clearly on the institutions, organizations, and individual managers who choose to use the technology. Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions. Third, in an ethical, political society, individuals and others can recover damages done to them through a set of laws characterized by due process.

ETHICAL ANALYSIS

When confronted with a situation that seems to present ethical issues, how should you analyze it? The following five-step process should help.

1. *Identify and describe clearly the facts*. Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.
2. *Define the conflict or dilemma and identify the higher-order values involved*. Ethical, social, and political issues always reference higher values. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). Typically, an ethical issue involves a dilemma: two diametrically opposed courses of action that support worthwhile values. For example, the chapter-ending case study illustrates two competing values: the need to protect citizens from terrorist acts and the need to protect individual privacy.
3. *Identify the stakeholders*. Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.
4. *Identify the options that you can reasonably take*. You may find that none of the options satisfy all the interests involved, but that some options do a better job than others. Sometimes arriving at a good or ethical solution may not always be a balancing of consequences to stakeholders.
5. *Identify the potential consequences of your options*. Some options may be ethically correct but disastrous from other points of view. Other options may work in one instance but not in other similar instances. Always ask yourself, "What if I choose this option consistently over time?"

CANDIDATE ETHICAL PRINCIPLES

Once your analysis is complete, what ethical principles or rules should you use to make a decision? What higher-order values should inform your judgment? Although you are the only one who can decide which among many ethical principles you will follow, and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history.

1. Do unto others as you would have them do unto you (the **Golden Rule**). Putting yourself into the place of others, and thinking of yourself as the object of the decision, can help you think about fairness in decision making.
2. If an action is not right for everyone to take, it is not right for anyone **(Immanuel Kant's Categorical Imperative)**. Ask yourself, "If everyone did this, could the organization, or society, survive?"
3. If an action cannot be taken repeatedly, it is not right to take at all **(Descartes' rule of change)**. This is the slippery-slope rule: An action may bring about a small change now that is acceptable, but if it is repeated, it would bring unacceptable changes in the long run. In the vernacular, it might be stated as "once started down a slippery path, you may not be able to stop."
4. Take the action that achieves the higher or greater value (the **Utilitarian Principle**). This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
5. Take the action that produces the least harm or the least potential cost (**Risk Aversion Principle**). Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid these high-failure-cost actions, paying greater attention obviously to high-failure-cost potential of moderate to high probability.
6. Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the **ethical "no free lunch" rule**.) If something someone else has created is useful to you, it has value, and you should assume the creator wants compensation for this work.

Although these ethical rules cannot be guides to action, actions that do not easily pass these rules deserve some very close attention and a great deal of caution. The appearance of unethical behavior may do as much harm to you and your company as actual unethical behavior.

PROFESSIONAL CODES OF CONDUCT

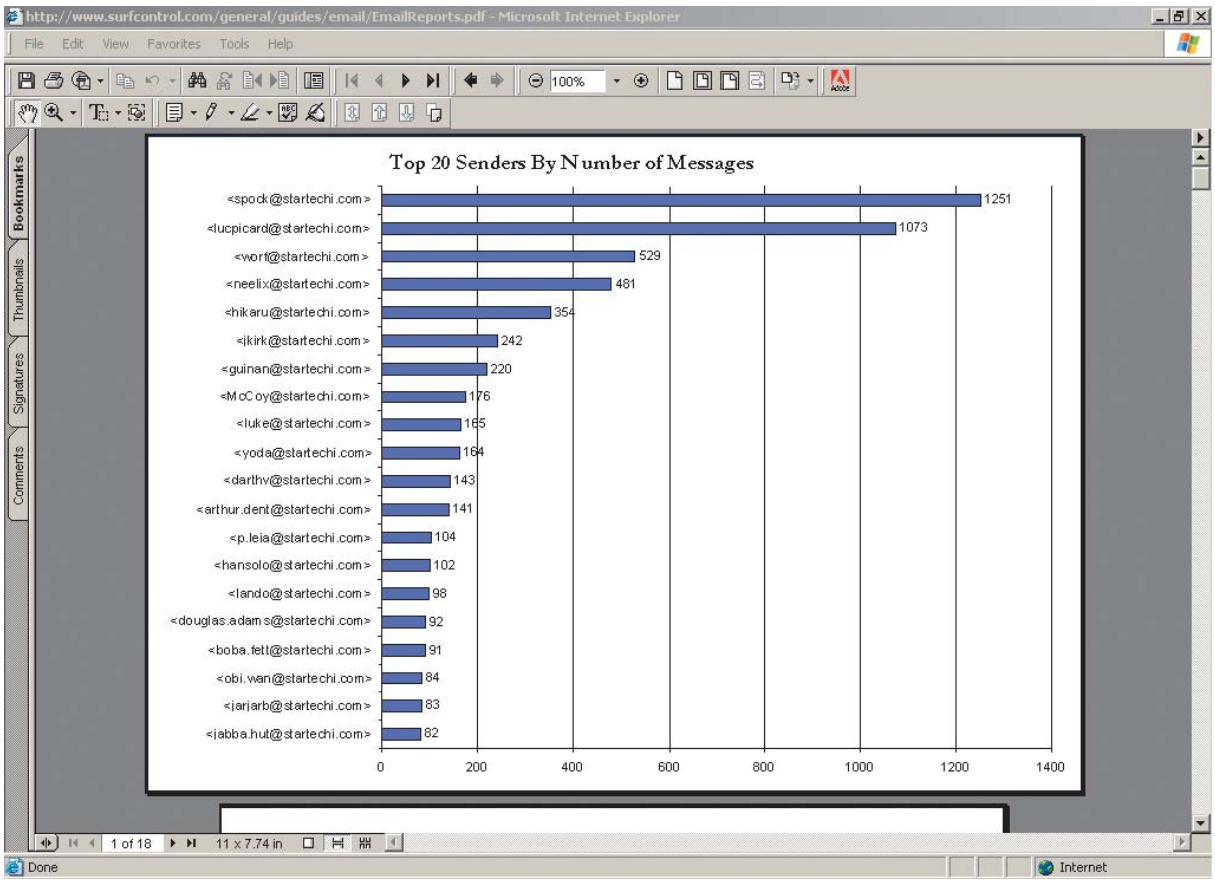
When groups of people claim to be professionals, they take on special rights and obligations because of their special claims to knowledge, wisdom, and respect. Professional codes of conduct are promulgated by associations of professionals, such as the American Medical Association (AMA), the American Bar Association (ABA), the Association of Information Technology Professionals (AITP), and the Association of Computing Machinery (ACM). These professional groups take responsibility for the partial regulation of their professions by determining entrance qualifications and competence. Codes of ethics are promises by professions to regulate themselves in the general interest of society. For example, avoiding harm to others, honoring property rights (including intellectual property), and respecting privacy are

among the General Moral Imperatives of the ACM's Code of Ethics and Professional Conduct.

SOME REAL-WORLD ETHICAL DILEMMAS

Information systems have created new ethical dilemmas in which one set of interests is pitted against another. For example, many of the large telephone companies in the United States are using information technology to reduce the sizes of their workforces. Voice recognition software reduces the need for human operators by enabling computers to recognize a customer's responses to a series of computerized questions. Many companies monitor what their employees are doing on the Internet to prevent them from wasting company resources on nonbusiness activities (see the Chapter 7 Interactive Session on Management).

In each instance, you can find competing values at work, with groups lined up on either side of a debate. A company may argue, for example, that it has a right to use information systems to increase productivity and reduce the size of its workforce to lower costs and stay in business. Employees displaced by information systems may argue that employers have some responsibility for their welfare. Business owners might feel obligated to monitor employee e-mail and Internet use to minimize drains on productivity. Employees might believe they should be able to use the Internet for short personal tasks in place of the



SurfControl offers tools for tracking Web and e-mail activity and for filtering unauthorized e-mail and Web site content. The benefits of monitoring employee e-mail and Internet use should be balanced with the need to respect employee privacy.

telephone. A close analysis of the facts can sometimes produce compromised solutions that give each side "half a loaf." Try to apply some of the principles of ethical analysis described to each of these cases. What is the right thing to do?

4.3 The Moral Dimensions of Information Systems

In this section, we take a closer look at the five moral dimensions of information systems first described in Figure 4-1. In each dimension we identify the ethical, social, and political levels of analysis and use real-world examples to illustrate the values involved, the stakeholders, and the options chosen.

INFORMATION RIGHTS: PRIVACY AND FREEDOM IN THE INTERNET AGE

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance (Ball, 2001). Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

The claim to privacy is protected in the U.S., Canadian, and German constitutions in a variety of different ways and in other countries through various statutes. In the United States, the claim to privacy is protected primarily by the First Amendment guarantees of freedom of speech and association, the Fourth Amendment protections against unreasonable search and seizure of one's personal documents or home, and the guarantee of due process.

Table 4-3 describes the major U.S. federal statutes that set forth the conditions for handling information about individuals in such areas as credit reporting, education, financial records, newspaper records, and electronic communications. The Privacy Act of 1974 has been the most important of these laws, regulating the federal government's collection, use, and disclosure of information. At present, most U.S. federal privacy laws apply only to the federal government and regulate very few areas of the private sector.

TABLE 4-3 FEDERAL PRIVACY LAWS IN THE UNITED STATES

GENERAL FEDERAL PRIVACY LAWS	PRIVACY LAWS AFFECTING PRIVATE INSTITUTIONS
Freedom of Information Act of 1966 as Amended (5 USC 552)	Fair Credit Reporting Act of 1970
Privacy Act of 1974 as Amended (5 USC 552a)	Family Educational Rights and Privacy Act of 1974
Electronic Communications Privacy Act of 1986	Right to Financial Privacy Act of 1978
Computer Matching and Privacy Protection Act of 1988	Privacy Protection Act of 1980
Computer Security Act of 1987	Cable Communications Policy Act of 1984
Federal Managers Financial Integrity Act of 1982	Electronic Communications Privacy Act of 1986
Driver's Privacy Protection Act of 1994	Video Privacy Protection Act of 1988
E-Government Act of 2002	The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
	Children's Online Privacy Protection Act of 1998 (COPPA)
	Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999

Most American and European privacy law is based on a regime called Fair Information Practices (FIP) first set forth in a report written in 1973 by a federal government advisory committee (U.S. Department of Health, Education, and Welfare, 1973). **Fair Information Practices (FIP)** is a set of principles governing the collection and use of information about individuals. FIP principles are based on the notion of a mutuality of interest between the record holder and the individual. The individual has an interest in engaging in a transaction, and the record keeper—usually a business or government agency—requires information about the individual to support the transaction. Once information is gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, the Federal Trade Commission (FTC) restated and extended the original FIP to provide guidelines for protecting online privacy. Table 4-4 describes the FTC's Fair Information Practice principles.

The FTC's FIP are being used as guidelines to drive changes in privacy legislation. In July 1998, the U.S. Congress passed the Children's Online Privacy Protection Act (COPPA), requiring Web sites to obtain parental permission before collecting information on children under the age of 13. The FTC has recommended additional legislation to protect online consumer privacy in advertising networks that collect records of consumer Web activity to develop detailed profiles, which are then used by other companies to target online ads. Other proposed Internet privacy legislation focuses on protecting the online use of personal identification numbers, such as social security numbers; protecting personal information collected on the Internet that deals with individuals not covered by the Children's Online Privacy Protection Act of 1998; and limiting the use of data mining for homeland security (see the chapter-ending case study).

Privacy protections have also been added to recent laws deregulating financial services and safeguarding the maintenance and transmission of health information about individuals. The Gramm-Leach-Bliley Act of 1999, which repeals earlier restrictions on affiliations among banks, securities firms, and insurance companies, includes some privacy protection for consumers of financial services. All financial institutions are required to disclose their policies and practices for protecting the privacy of nonpublic personal information and to allow customers to opt out of information-sharing arrangements with nonaffiliated third parties.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which took effect on April 14, 2003, includes privacy protection for medical records. The law gives patients access to their personal medical records

TABLE 4-4 FEDERAL TRADE COMMISSION FAIR INFORMATION PRACTICE PRINCIPLES

1. *Notice/awareness (core principle).* Web sites must disclose their information practices before collecting data. Includes identification of collector; uses of data; other recipients of data; nature of collection (active/inactive); voluntary or required status; consequences of refusal; and steps taken to protect confidentiality, integrity, and quality of the data.
2. *Choice/consent (core principle).* There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties.
3. *Access/participation.* Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
4. *Security.* Data collectors must take responsible steps to assure that consumer information is accurate and secure from unauthorized use.
5. *Enforcement.* There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulations.

maintained by healthcare providers, hospitals, and health insurers and the right to authorize how protected information about themselves can be used or disclosed. Doctors, hospitals, and other healthcare providers must limit the disclosure of personal information about patients to the minimum amount necessary to achieve a given purpose.

The European Directive on Data Protection

In Europe, privacy protection is much more stringent than in the United States. Unlike the United States, European countries do not allow businesses to use personally identifiable information without consumers' prior consent. On October 25, 1998, the European Commission's Directive on Data Protection went into effect, broadening privacy protection in the European Union (EU) nations. The directive requires companies to inform people when they collect information about them and disclose how it will be stored and used. Customers must provide their informed consent before any company can legally use data about them, and they have the right to access that information, correct it, and request that no further data be collected. **Informed consent** can be defined as consent given with knowledge of all the facts needed to make a rational decision. EU member nations must translate these principles into their own laws and cannot transfer personal data to countries, such as the United States, that do not have similar privacy protection regulations.

Working with the European Commission, the U.S. Department of Commerce developed a safe harbor framework for U.S. firms. A **safe harbor** is a private, self-regulating policy and enforcement mechanism that meets the objectives of government regulators and legislation but does not involve government regulation or enforcement.

U.S. businesses doing business with Europeans are allowed to use personal data from EU countries if they develop privacy protection policies that meet EU standards. Enforcement occurs in the United States using self-policing, regulation, and government enforcement of fair trade statutes. Firms must be certified by public accounting firms to be "safe harbor" for personal data on Europeans, and this certification is recognized (but not enforced) by the Department of Commerce. With this safe harbor policy, the Americans and Europeans have been able to overcome their differences on privacy matters, and permit trade to take place.

Internet Challenges to Privacy

Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it.

It is possible to record all online activities of literally tens of millions of people, including which online newsgroups or files a person has accessed, which Web sites and Web pages he or she has visited, and what items that person has inspected or purchased over the Web. Much of this monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. Tools to monitor visits to the World Wide Web have become popular because they help organizations determine who is visiting their Web sites and how to better target their offerings. Some firms also monitor the Internet usage of their employees to see how they are using company network resources. Web retailers now have access to software that lets them "watch" the online shopping behavior of individuals and groups while they are visiting a Web site

and making purchases. The commercial demand for this personal information is virtually insatiable.

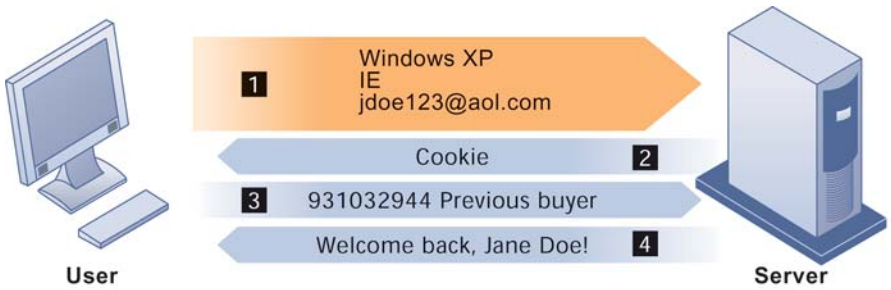
Web sites can learn the identities of their visitors if the visitors voluntarily register at the site to purchase a product or service or to obtain a free service, such as information. Web sites can also capture information about visitors without their knowledge using cookie technology.

Cookies are tiny files deposited on a computer hard drive when a user visits certain Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie, depending on the activity during the visit. In this way, the site can customize its contents for each visitor's interests. For example, if you purchase a book on the Amazon.com Web site and return later from the same browser, the site will welcome you by name and recommend other books of interest based on your past purchases. DoubleClick, described earlier in this chapter, uses cookies to build its dossiers with details of online purchases and to examine the behavior of Web site visitors. Figure 4-3 illustrates how cookies work.

Web sites using cookie technology cannot directly obtain visitors' names and addresses. However, if a person has registered at a site, that information can be combined with cookie data to identify the visitor. Web site owners can also combine the data they have gathered from cookies and other Web site monitoring tools with personal data from other sources, such as offline data collected from surveys or paper catalog purchases, to develop very detailed profiles of their visitors.

There are now even more subtle and surreptitious tools for surveillance of Internet users. Marketers use **Web bugs** as another tool to monitor online behavior. Web bugs are tiny graphic files embedded in e-mail messages and Web pages that are designed to monitor who is reading the e-mail message or Web page and transmit that information to another computer. Other **spyware** can secretly install itself on an Internet user's computer by piggybacking on larger

FIGURE 4-3 HOW COOKIES IDENTIFY WEB VISITORS



1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

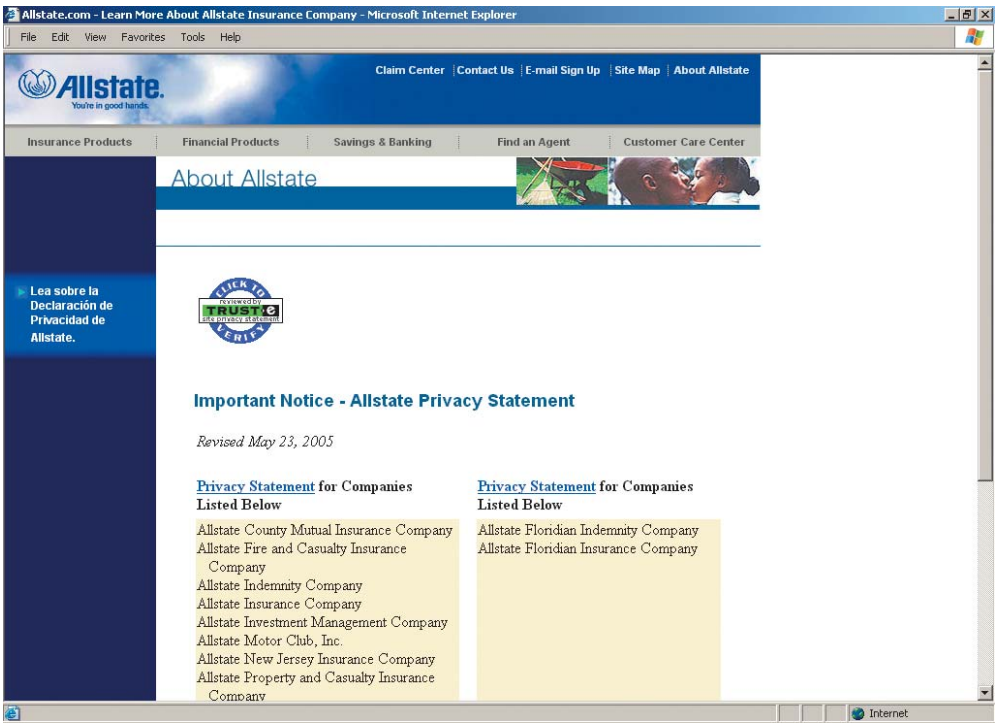
Cookies are written by a Web site on a visitor's hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

applications. Once installed, the spyware calls out to Web sites to send banner ads and other unsolicited material to the user, and it can also report the user's movements on the Internet to other computers. Spyware also can log user keystrokes and send the information to other sites on the Web without the user's knowledge. More information is available about Web bugs, spyware, and other intrusive software in Chapter 7.

Google has been using tools to scan the contents of messages received by users of its free Web-based e-mail service called Gmail. Ads that users see when they read their e-mail are related to the subjects of these messages. Google's service offers users 1 gigabyte of storage space—far more than any of its competitors—but privacy advocates find the practice offensive.

The United States has allowed businesses to gather transaction information generated in the marketplace and then use that information for other marketing purposes without obtaining the informed consent of the individual whose information is being used. U.S. e-commerce sites are largely content to publish statements on their Web sites informing visitors about how their information will be used. Some have added opt-out selection boxes to these information policy statements. An **opt-out** model of informed consent permits the collection of personal information until the consumer specifically requests that the data not be collected. Privacy advocates would like to see wider use of an **opt-in** model of informed consent in which a business is prohibited from collecting any personal information unless the consumer specifically takes action to approve information collection and use.

The online industry has preferred self-regulation to privacy legislation for protecting consumers. In 1998, the online industry formed the Online Privacy Alliance to encourage self-regulation to develop a set of privacy guidelines for its members. The group promotes the use of online seals, such as that of TRUSTe, certifying Web sites adhering to certain privacy principles. Members of the advertising network industry, including DoubleClick, have created an



Web sites are posting their privacy policies for visitors to review. The TRUSTe seal designates Web sites that have agreed to adhere to TRUSTe's established privacy principles of disclosure, choice, access, and security.

additional industry association called the Network Advertising Initiative (NAI) to develop its own privacy policies to help consumers opt out of advertising network programs and provide consumers redress from abuses.

While nearly all the top 100 Web sites have privacy policies, you will quickly discover upon reading them that there are few limitations these firms place on their use of your personal information. In turn, consumers do not do as much as they could or should to protect themselves. Many companies with Web sites do not have privacy policies. Of the companies that do post privacy polices on their Web sites, about half do not monitor their sites to ensure they adhere to these policies. While the vast majority of online customers claim they are concerned about online privacy, less than half read the privacy statements on Web sites (Laudon and Traver, 2006).

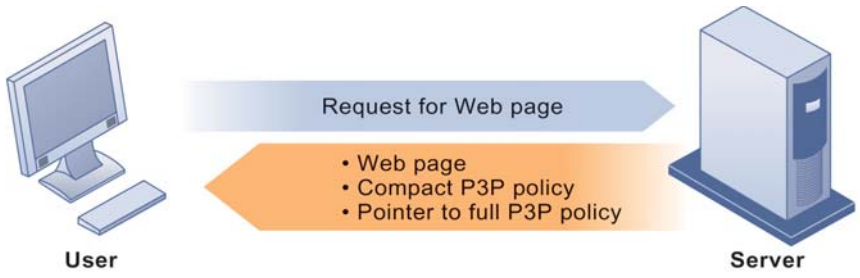
Technical Solutions

In addition to legislation, new technologies are available to protect user privacy during interactions with Web sites. Many of these tools are used for encrypting e-mail, for making e-mail or surfing activities appear anonymous, for preventing client computers from accepting cookies, or for detecting and eliminating spyware.

There are now tools to help users determine the kind of personal data that can be extracted by Web sites. The Platform for Privacy Preferences, known as P3P, enables automatic communication of privacy policies between an e-commerce site and its visitors. **P3P** provides a standard for communicating a Web site's privacy policy to Internet users and for comparing that policy to the user's preferences or to other standards, such as the FTC's new FIP guidelines or the European Directive on Data Protection. Users can use P3P to select the level of privacy they wish to maintain when interacting with the Web site.

The P3P standard allows Web sites to publish privacy policies in a form that computers can understand. Once it is codified according to P3P rules, the privacy policy becomes part of the software for individual Web pages (see Figure 4-4). Users of Microsoft Internet Explorer Web browsing software

FIGURE 4-4 THE P3P STANDARD



1. The user with P3P Web browsing software requests a Web page.
2. The Web server returns the Web page along with a compact version of the Web site's policy and a pointer to the full P3P policy. If the Web site is not P3P compliant, no P3P data are returned.
3. The user's Web browsing software compares the response from the Web site with the user's privacy preferences. If the Web site does not have a P3P policy or the policy does not match the privacy levels established by the user, it warns the user or rejects the cookies from the Web site. Otherwise, the Web page loads normally.

P3P enables Web sites to translate their privacy policies into a standard format that can be read by the user's Web browser software. The user's Web browser software evaluates the Web site's privacy policy to determine whether it is compatible with the user's privacy preferences.

can access and read the P3P site's privacy policy and a list of all cookies coming from the site. Internet Explorer enables users to adjust their computers to screen out all cookies or let in selected cookies based on specific levels of privacy. For example, the "medium" level accepts cookies from first-party host sites that have opt-in or opt-out policies but rejects third-party cookies that use personally identifiable information without an opt-in policy.

However, P3P only works with Web sites of members of the World Wide Web Consortium who have translated their Web site privacy policies into P3P format. The technology will display cookies from Web sites that are not part of the consortium, but users will not be able to obtain sender information or privacy statements. Many users may also need to be educated about interpreting company privacy statements and P3P levels of privacy.

PROPERTY RIGHTS: INTELLECTUAL PROPERTY

Contemporary information systems have severely challenged existing law and social practices that protect private intellectual property. **Intellectual property** is considered to be intangible property created by individuals or corporations. Information technology has made it difficult to protect intellectual property because computerized information can be so easily copied or distributed on networks. Intellectual property is subject to a variety of protections under three different legal traditions: trade secrets, copyright, and patent law.

Trade Secrets

Any intellectual work product—a formula, device, pattern, or compilation of data-used for a business purpose can be classified as a **trade secret**, provided it is not based on information in the public domain. Protections for trade secrets vary from state to state. In general, trade secret laws grant a monopoly on the ideas behind a work product, but it can be a very tenuous monopoly.

Software that contains novel or unique elements, procedures, or compilations can be included as a trade secret. Trade secret law protects the actual ideas in a work product, not only their manifestation. To make this claim, the creator or owner must take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.

The limitation of trade secret protection is that, although virtually all software programs of any complexity contain unique elements of some sort, it is difficult to prevent the ideas in the work from falling into the public domain when the software is widely distributed.

Copyright

Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death. For corporate-owned works, copyright protection lasts for 95 years after their initial creation. Congress has extended copyright protection to books, periodicals, lectures, dramas, musical compositions, maps, drawings, artwork of any kind, and motion pictures. The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their laws.

In the mid-1960s, the Copyright Office began registering software programs, and in 1980 Congress passed the Computer Software Copyright Act, which clearly provides protection for software program code and for copies of the original sold in commerce, and sets forth the rights of the purchaser to use the software while the creator retains legal title.

Copyright protects against copying of entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback to copyright protection is that the underlying ideas behind a work are not protected, only their manifestation in a work. A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright.

"Look and feel" copyright infringement lawsuits are precisely about the distinction between an idea and its expression. For instance, in the early 1990s Apple Computer sued Microsoft Corporation and Hewlett-Packard for infringement of the expression of Apple's Macintosh interface, claiming that the defendants copied the expression of overlapping windows. The defendants countered that the idea of overlapping windows can be expressed only in a single way and, therefore, was not protectable under the merger doctrine of copyright law. When ideas and their expression merge, the expression cannot be copyrighted.

In general, courts appear to be following the reasoning of a 1989 case—Brown Bag Software vs. Symantec Corp.—in which the court dissected the elements of software alleged to be infringing. The court found that similar concept, function, general functional features (e.g., drop-down menus), and colors are not protectable by copyright law (*Brown Bag vs. Symantec Corp.*, 1992).

Patents

A **patent** grants the owner an exclusive monopoly on the ideas behind an invention for 20 years. The congressional intent behind patent law was to ensure that inventors of new machines, devices, or methods receive the full financial and other rewards of their labor and yet still make widespread use of the invention possible by providing detailed diagrams for those wishing to use the idea under license from the patent's owner. The granting of a patent is determined by the Patent Office and relies on court rulings.

The key concepts in patent law are originality, novelty, and invention. The Patent Office did not accept applications for software patents routinely until a 1981 Supreme Court decision that held that computer programs could be a part of a patentable process. Since that time, hundreds of patents have been granted and thousands await consideration.

The strength of patent protection is that it grants a monopoly on the underlying concepts and ideas of software. The difficulty is passing stringent criteria of nonobviousness (e.g., the work must reflect some special understanding and contribution), originality, and novelty, as well as years of waiting to receive protection.

Challenges to Intellectual Property Rights

Contemporary information technologies, especially software, pose severe challenges to existing intellectual property regimes and, therefore, create significant ethical, social, and political issues. Digital media differ from physical media like books, periodicals, CDs, and newspapers in terms of ease of replication; ease of transmission; ease of alteration; difficulty in classifying a software work as a program, book, or even music; compactness—making theft easy; and difficulties in establishing uniqueness.

The proliferation of electronic networks, including the Internet, has made it even more difficult to protect intellectual property. Before widespread use of networks, copies of software, books, magazine articles, or films had to be stored on physical media, such as paper, computer disks, or videotape, creating some hurdles to distribution. Using networks, information can be more widely reproduced and distributed. A study conducted by the International Data Corporation for the Business Software Alliance found that more than one-third of the software worldwide was counterfeit or pirated, and the Business Software Alliance reported $29 billion in yearly losses from software piracy (Geitner, 2004; Lohr, 2004).

The Internet was designed to transmit information freely around the world, including copyrighted information. With the World Wide Web in particular, you can easily copy and distribute virtually anything to thousands and even millions of people around the world, even if they are using different types of computer systems. Information can be illicitly copied from one place and distributed through other systems and networks even though these parties do not willingly participate in the infringement.

Individuals have been illegally copying and distributing digitized MP3 music files on the Internet for a number of years. File sharing services such as Napster, and later Grokster, Kazaa, and Morpheus sprung up to help users locate and swap digital music files, including those protected by copyright. Illegal file-sharing became so widespread that it threatened the viability of the music recording industry.

The recording industry won significant legal battles against Napster, and later against Grokster and all commercial P2P networks. The U.S. Supreme Court found in June 2005 that file-sharing networks that intentionally profited from illegal distribution of music could be held liable for their actions. This decision forced most of the large-scale commercial P2P networks to shut down, or to seek legal distribution agreements with the music publishers.

Despite these victories in court, illegal music file sharing abounds on the Internet: 27 percent of Internet users report downloading music from illegal sites (36 million Americans). This is down from a peak of 32 percent of Internet users downloading in 2002. The good news—if there is any in this area—is that legal music downloads from sites like iTunes has expanded to more than 43 percent of Internet users in the United States. (Madden and Rainie, 2005). As more and more homes adopt high-speed Internet access, illegal file sharing of videos will pose similar threats to the motion picture industry.

Mechanisms are being developed to sell and distribute books, articles, and other intellectual property legally on the Internet, and the **Digital Millennium Copyright Act (DMCA)** of 1998 is providing some copyright protection. The DMCA implemented a World Intellectual Property Organization Treaty that makes it illegal to circumvent technology-based protections of copyrighted materials. Internet service providers (ISPs) are required to take down sites of copyright infringers that they are hosting once they are notified of the problem.

Microsoft and 1,400 other software and information content firms are represented by the Software and Information Industry Association (SIIA), which lobbies for new laws and enforcement of existing laws to protect intellectual property around the world. (SIIA was formed on January 1, 1999, from the merger of the Software Publishers Association [SPA] and the Information Industry Association [IIA].) The SIIA runs an antipiracy hotline for individuals to report piracy activities and educational programs to help organizations combat software piracy and has published guidelines for employee use of software.

ACCOUNTABILITY, LIABILITY, AND CONTROL

Along with privacy and property laws, new information technologies are challenging existing liability law and social practices for holding individuals and institutions accountable. If a person is injured by a machine controlled, in part, by software, who should be held accountable and, therefore, held liable? Should a public bulletin board or an electronic service, such as AOL, permit the transmission of pornographic or offensive material (as broadcasters), or should they be held harmless against any liability for what users transmit (as is true of common carriers, such as the telephone system)? What about the Internet? If you outsource your information processing, can you hold the external vendor liable for injuries done to your customers? Some real-world examples may shed light on these questions.

Computer-Related Liability Problems

During the weekend of March 15, 2002, tens of thousands of Bank of America customers in California, Arizona, and Nevada were unable to use their paychecks and social security payments that had just been deposited electronically. Checks bounced. Withdrawals were blocked because of insufficient funds. Because of an operating error at the bank's computer center in Nevada, a batch of direct-deposit transactions was not processed. The bank lost track of money that should have been credited to customers' accounts, and it took days to rectify the problem (Carr and Gallagher, 2002). Who is liable for any economic harm caused to individuals or businesses that could not access their full account balances in this period?

This case reveals the difficulties faced by information systems executives who ultimately are responsible for any harm done by systems developed by their staffs. In general, insofar as computer software is part of a machine, and the machine injures someone physically or economically, the producer of the software and the operator can be held liable for damages. Insofar as the software acts like a book, storing and displaying information, courts have been reluctant to hold authors, publishers, and booksellers liable for contents (the exception being instances of fraud or defamation), and hence courts have been wary of holding software authors liable for booklike software.

In general, it is very difficult (if not impossible) to hold software producers liable for their software products when those products are considered like books are, regardless of the physical or economic harm that results. Historically, print publishers, books, and periodicals have not been held liable because of fears that liability claims would interfere with First Amendment rights guaranteeing freedom of expression.

What about software as service? ATM machines are a service provided to bank customers. Should this service fail, customers will be inconvenienced and perhaps harmed economically if they cannot access their funds in a timely manner. Should liability protections be extended to software publishers and operators of defective financial, accounting, simulation, or marketing systems?

Software is very different from books. Software users may develop expectations of infallibility about software; software is less easily inspected than a book, and it is more difficult to compare with other software products for quality; software claims actually to perform a task rather than describe a task, as a book does; and people come to depend on services essentially based on software. Given the centrality of software to everyday life, the chances are excellent that liability law will extend its reach to include software even when the software merely provides an information service.

Telephone systems have not been held liable for the messages transmitted because they are regulated common carriers. In return for their right to provide telephone service, they must provide access to all, at reasonable rates, and achieve acceptable reliability. But broadcasters and cable television systems are subject to a wide variety of federal and local constraints on content and facilities. Organizations can be held liable for offensive content on their Web sites; and online services, such as Prodigy or AOL, might be held liable for postings by their users. Although U.S. courts have increasingly exonerated Web sites and ISPs for posting material by third parties, the threat of legal action still has a chilling effect on small companies or individuals who cannot afford to take their cases to trial.

SYSTEM QUALITY: DATA QUALITY AND SYSTEM ERRORS

The debate over liability and accountability for unintentional consequences of system use raises a related but independent moral dimension: What is an acceptable, technologically feasible level of system quality? At what point should system managers say, "Stop testing, we've done all we can to perfect this software. Ship it!" Individuals and organizations may be held responsible for avoidable and foreseeable consequences, which they have a duty to perceive and correct. And the gray area is that some system errors are foreseeable and correctable only at very great expense, an expense so great that pursuing this level of perfection is not feasible economically—no one could afford the product.

For example, although software companies try to debug their products before releasing them to the marketplace, they knowingly ship buggy products because the time and cost of fixing all minor errors would prevent these products from ever being released. What if the product was not offered on the marketplace, would social welfare as a whole not advance and perhaps even decline? Carrying this further, just what is the responsibility of a producer of computer services—should it withdraw the product that can never be perfect, warn the user, or forget about the risk (let the buyer beware)?

Three principal sources of poor system performance are (1) software bugs and errors, (2) hardware or facility failures caused by natural or other causes, and (3) poor input data quality. Chapter 10 discusses why zero defects in software code of any complexity cannot be achieved and why the seriousness of remaining bugs cannot be estimated. Hence, there is a technological barrier to perfect software, and users must be aware of the potential for catastrophic failure. The software industry has not yet arrived at testing standards for producing software of acceptable but not perfect performance.

Although software bugs and facility catastrophes are likely to be widely reported in the press, by far the most common source of business system failure is data quality. Few companies routinely measure the quality of their data, but studies of individual organizations report data error rates ranging from 0.5 to 30 percent (Gilhooly, 2005).

QUALITY OF LIFE: EQUITY, ACCESS, AND BOUNDARIES

The negative social costs of introducing information technologies and systems are beginning to mount along with the power of the technology. Many of these negative social consequences are not violations of individual rights or property

crimes. Nevertheless, these negative consequences can be extremely harmful to individuals, societies, and political institutions. Computers and information technologies potentially can destroy valuable elements of our culture and society even while they bring us benefits. If there is a balance of good and bad consequences of using information systems, who do we hold responsible for the bad consequences? Next, we briefly examine some of the negative social consequences of systems, considering individual, social, and political responses.

Balancing Power: Center Versus Periphery

An early fear of the computer age was that huge, centralized mainframe computers would centralize power at corporate headquarters and in the nation's capital, resulting in a Big Brother society, as was suggested in George Orwell's novel *1984*. The shift toward highly decentralized computing, coupled with an ideology of empowerment of thousands of workers, and the decentralization of decision making to lower organizational levels have reduced the fears of power centralization in institutions. Yet much of the empowerment described in popular business magazines is trivial. Lower-level employees may be empowered to make minor decisions, but the key policy decisions may be as centralized as in the past.

Rapidity of Change: Reduced Response Time to Competition

Information systems have helped to create much more efficient national and international markets. The now-more-efficient global marketplace has reduced the normal social buffers that permitted businesses many years to adjust to competition. Time-based competition has an ugly side: The business you work for may not have enough time to respond to global competitors and may be wiped out in a year, along with your job. We stand the risk of developing a "just-in-time society" with "just-in-time jobs" and "just-in-time" workplaces, families, and vacations.

Maintaining Boundaries: Family, Work, and Leisure

Parts of this book were produced on trains and planes, as well as on family vacations and during what otherwise might have been "family" time. The danger to ubiquitous computing, telecommuting, nomad computing, and the "do anything anywhere" computing environment is that it might actually come true. If so, the traditional boundaries that separate work from family and just plain leisure will be weakened.

Although authors have traditionally worked just about anywhere (typewriters have been portable for nearly a century), the advent of information systems, coupled with the growth of knowledge-work occupations, means that more and more people will be working when traditionally they would have been playing or communicating with family and friends. The work umbrella now extends far beyond the eight-hour day.

Even leisure time spent on the computer threatens these close social relationships. Extensive Internet use, even for entertainment or recreational purposes, takes people away from their family and friends. The Interactive Session on Organizations explores what happens to children and teenagers when time spent online is excessive or inappropriate.

Weakening these institutions poses clear-cut risks. Family and friends historically have provided powerful support mechanisms for individuals, and they act as balance points in a society by preserving private life, providing a

INTERACTIVE SESSION: ORGANIZATIONS

THE INTERNET: FRIEND OR FOE TO CHILDREN?

The Internet has so much to offer people of all ages, including children. School-age children typically use the Internet for school assignments, for downloading music, playing games, and for connecting with others. A child might use e-mail or instant messaging to stay in touch with friends who have moved away or family members in distant locations. Shy children may find an online community and set of "friends" with whom to share feelings that they are unable to express in person. Children living in rural areas can stay in touch with others who are isolated geographically.

But there's a dark side to all that Internet use. It can also socially isolate children and expose them to unhealthy activities and experiences.

According to child and adolescent psychiatrist Dr. David Bassler, certain children become too isolated as a result of heavy Internet use. A shy or overweight child can become a football star in an online game or a persona in MySpace. Bassler believes that "a degree of this is healthy, but if it starts to become the primary focus, it can become a problem." Staying online for long periods of time may make a shy or depressed child even more shy or depressed.

When children spend too much time online, they don't do their homework or can't focus on their work in school because their online activities have drained their energy. They miss out on sports and other activities and they don't spend enough time with their real-world peers and family members.

E-mail and instant messaging can help youngsters stay in touch with friends and family but they have also become instruments for "cyberbullying." Kids will use these tools to send insulting remarks to each other or to distribute personal details meant for a few close friends to a wide circle of strangers. One 16-year-old boy whose girlfriend had broken up with him over the telephone was shocked to find a detailed explanation for her actions on her instant messenger profile. She had used instant messaging to tell their entire network of social contacts, including friends of friends in different high schools, details about the reasons for the breakup. They boy was so upset he skipped school the next day.

Ten million young people use the Internet each day, and one in five have been solicited or approached by a child predator, according to the FBI. Federal arrests for online exploitation of children doubled from 863 to 1,649 between 2003 and 2005. Fifty percent of child victims of online sex abuse are in the seventh through ninth grades.

Online predators monitor screen names and scrutinize personal information on social networking sites such as MySpace, Friendster, and Facebook to find youngsters with self-esteem problems. They'll ask youngsters questions such as "Do you like this band? Can I help you with your homework?" Then they'll try to arrange a physical meeting with these juveniles.

Dr. Robert Kraut, a professor at Carnegie-Mellon University who has studied online behavior for more than a decade, found that the more people use the Internet, the less they socialize and the less they communicate with family members. High Internet usage among teenagers is associated with a decline in social support. Many hours spent online in casual conversation with other strangers don't translate into meaningful relationships.

Obesity, now an epidemic in the United States, is especially prevalent among youngsters who sit at their computers for hours at a time munching on snack food. And there are plenty of Web sites encouraging them to do just that.

Food companies aggressively use Internet games and other perks such as screen-saver downloads to entice children into buying their brands. Their Web sites offer childrens' games linked to snacks, such as Chips Ahoy Soccer Shootout, Pop-Tart Slalom, and Lucky Charms Wild Chocolate Mine. A Kaiser Family Foundation study found that between June and November 2005 more than 12.2 million children had visited 77 food company Web sites it examined.

According to the study's lead researcher Vicky Rideout, Internet advertising "still doesn't have the reach TV advertising has. But who it does reach, it reaches more deeply." This study is the first to investigate the scope of Internet advertising aimed at children.

Sources: Johanna Ambrosio, "Connected to Nowhere," *Information Week*, May 1, 2006; Jennifer B. McKim, "Keep Your Child Safe from Online Predators," *Orange County Register*, July 18, 2006; and Curtis L. Taylor, "Kids Swallowing Online Food Company Lures," *Newsday*, July 20, 2006.

CASE STUDY QUESTIONS

1. Does use of the Internet by children and teenagers pose an ethical dilemma? Why or why not?
2. Should parents restrict use of the Internet by children or teenagers? Why or why not?

MIS IN ACTION

Visit Nabiscoworld.com or another Web site from a food company that features games or other interactive features of interest to children and teenagers. Explore the site and answer the following questions.

1. What kinds of games and interactive features are available at this site? Are there any restrictions on who can play?
2. How do these sites help the company pitch food products to children?
3. Do these sites collect personal information? What kind of information?
4. Are these sites at all beneficial to consumers? What are the benefits?
5. Do these sites represent an ethical dilemma? Why or why not?

place for people to collect their thoughts, allowing people to think in ways contrary to their employer, and dream.

Dependence and Vulnerability

Today, our businesses, governments, schools, and private associations, such as churches, are incredibly dependent on information systems and are, therefore, highly vulnerable if these systems fail. With systems now as ubiquitous as the telephone system, it is startling to remember that there are no regulatory or standard-setting forces in place that are similar to telephone, electrical, radio, television, or other public-utility technologies. The absence of standards and the criticality of some system applications will probably call forth demands for national standards and perhaps regulatory oversight.

Computer Crime and Abuse

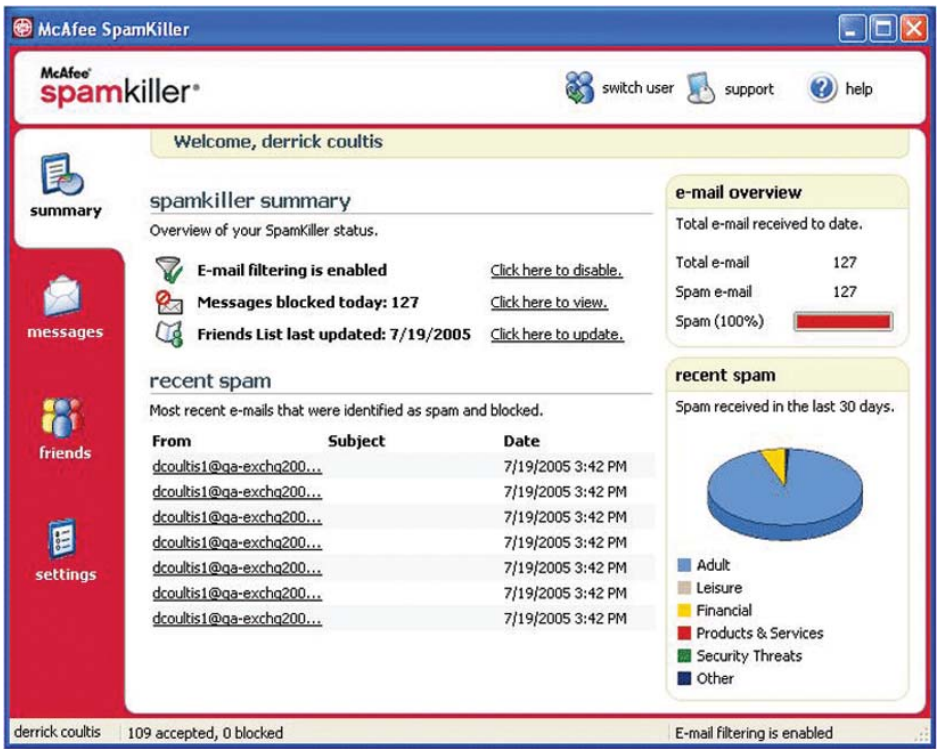
New technologies, including computers, create new opportunities for committing crime by creating new valuable items to steal, new ways to steal them, and new ways to harm others. **Computer crime** is the commission of illegal acts through the use of a computer or against a computer system. Computers or computer systems can be the object of the crime (destroying a company's computer center or a company's computer files), as well as the instrument of a crime (stealing computer lists by illegally gaining access to a computer system using a home computer). Simply accessing a computer system without authorization or with intent to do harm, even by accident, is now a federal crime.

Computer abuse is the commission of acts involving a computer that may not be illegal but that are considered unethical. The popularity of the Internet and e-mail has turned one form of computer abuse—spamming—into a serious problem for both individuals and businesses. **Spam** is junk e-mail sent by an organization or individual to a mass audience of Internet users who have expressed no interest in the product or service being marketed. Spammers tend

Although some people enjoy the convenience of working at home, the do-anything-anywhere computing environment can blur the traditional boundaries between work and family time.

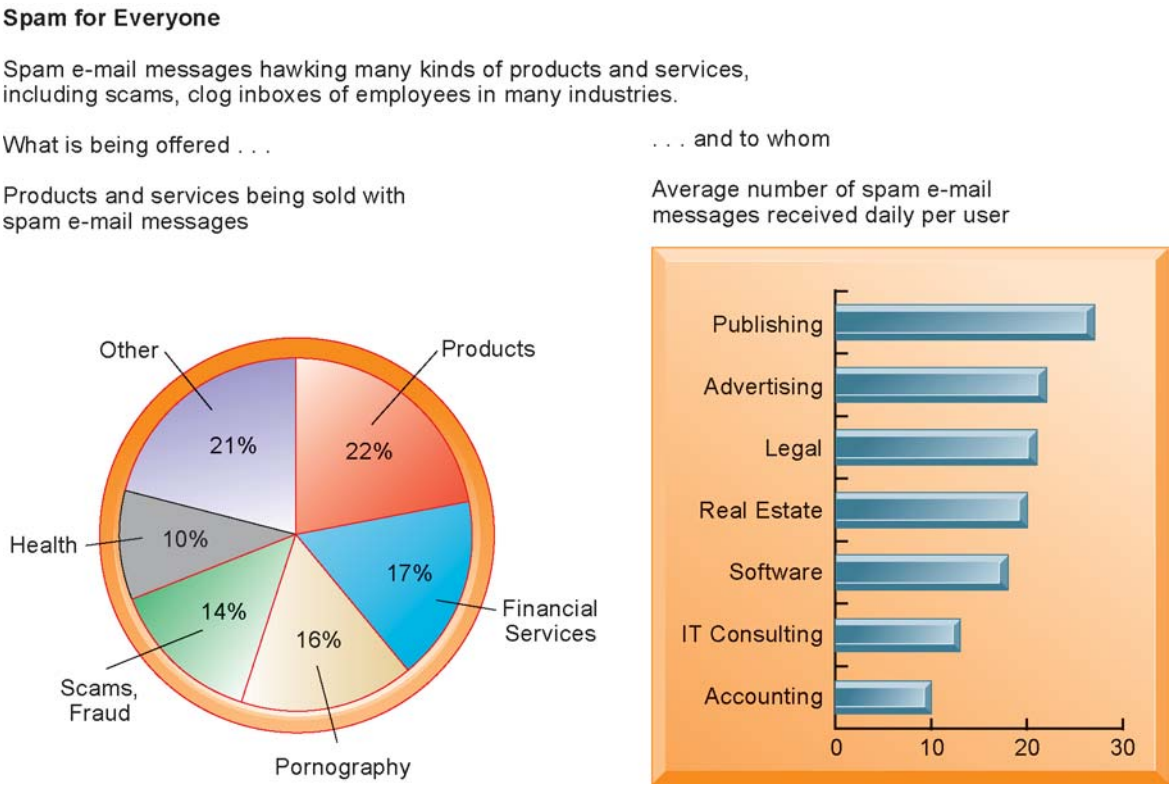
to market pornography, fraudulent deals and services, outright scams, and other products not widely approved in most civilized societies. Some countries have passed laws to outlaw spamming or to restrict its use. In the United States, it is still legal if it does not involve fraud and the sender and subject of the e-mail are properly identified.

Spamming has mushroomed because it only costs a few cents to send thousands of messages advertising wares to Internet users. Hundreds of CDs for sale on the Web offer spammers millions of e-mail addresses harvested by software robots that read message boards, chat rooms, and Web sites, or spammers use their own harvesting tools for this purpose. Spam now accounts for 70 percent of Internet e-mail traffic worldwide. Figure 4-5 provides data on



Spam consists of unsolicited e-mail messages, which can be bothersome, offensive, and even a drain on office worker productivity. Spam filtering software such as McAfee's SpamKiller blocks suspicious e-mail.

FIGURE 4-5 THE SPAMMING PROBLEM



This figure shows the major types of products and services hawked through spam e-mail messages and the industries that receive the most spam.

the scope of spamming and the types of industries most affected by the practice.

Spam costs for businesses are very high (an estimated $50 billion per year) because of the computing and network resources consumed by billions of unwanted e-mail messages and the time required to deal with them. Internet service providers and individuals can combat spam by using spam filtering software to block suspicious e-mail before it enters a recipient's e-mail inbox. However, spam filters may block legitimate messages, and many spammers skirt around filters by continually changing their e-mail accounts. Many spam messages are sent from one country while another country hosts the spam Web site.

Spamming is more tightly regulated in Europe than in the United States. On May 30, 2002, the European Parliament passed a ban on unsolicited commercial messaging. Electronic marketing can be targeted only to people who have given prior consent.

The U.S. CAN-SPAM Act of 2003, which went into effect on January 1, 2004, does not outlaw spamming but does ban deceptive e-mail practices by requiring commercial e-mail messages to display accurate subject lines, identify the true senders, and offer recipients an easy way to remove their names from e-mail lists. It also prohibits the use of fake return addresses. A few people have been prosecuted under the law, but spamming increased since it went into effect.

Employment: Trickle-Down Technology and Reengineering Job Loss

Reengineering work is typically hailed in the information systems community as a major benefit of new information technology. It is much less frequently noted that redesigning business processes could potentially cause millions of mid-level managers and clerical workers to lose their jobs. One economist has raised the possibility that we will create a society run by a small "high tech elite of corporate professionals . . . in a nation of the permanently unemployed" (Rifkin, 1993).

Other economists are much more sanguine about the potential job losses. They believe relieving bright, educated workers from reengineered jobs will result in these workers moving to better jobs in fast-growth industries. Missing from this equation are unskilled, blue-collar workers and older, less well-educated middle managers. It is not clear that these groups can be retrained easily for high-quality (high-paying) jobs. Careful planning and sensitivity to employee needs can help companies redesign work to minimize job losses.

Equity and Access: Increasing Racial and Social Class Cleavages

Does everyone have an equal opportunity to participate in the digital age? Will the social, economic, and cultural gaps that exist in the United States and other societies be reduced by information systems technology? Or will the cleavages be increased, permitting the better off to become even more better off relative to others?

These questions have not yet been fully answered because the impact of systems technology on various groups in society has not been thoroughly studied. What is known is that information, knowledge, computers, and access to these resources through educational institutions and public libraries are inequitably distributed along ethnic and social class lines, as are many other information resources. Several studies have found that certain ethnic and income groups in the United States are less likely to have computers or online Internet access even though computer ownership and Internet access have soared in the past five years. Although the gap is narrowing, higher-income families in each ethnic group are still more likely to have home computers and Internet access than lower-income families in the same group.

A similar **digital divide** exists in U.S. schools, with schools in high-poverty areas less likely to have computers, high-quality educational technology programs, or Internet access availability for their students. Left uncorrected, the digital divide could lead to a society of information haves, computer literate and skilled, versus a large group of information have-nots, computer illiterate and unskilled. Public interest groups want to narrow this digital divide by making digital information services—including the Internet—available to virtually everyone, just as basic telephone service is now.

Health Risks: RSI, CVS, and Technostress

The most important occupational disease today is **repetitive stress injury (RSI)**. RSI occurs when muscle groups are forced through repetitive actions often with high-impact loads (such as tennis) or tens of thousands of repetitions under low-impact loads (such as working at a computer keyboard).

The single largest source of RSI is computer keyboards. The most common kind of computer-related RSI is **carpal tunnel syndrome (CTS)**, in which pressure on the median nerve through the wrist's bony structure, called a

Repetitive stress injury (RSI) is the leading occupational disease today. The single largest cause of RSI is computer keyboard work.

carpal tunnel, produces pain. The pressure is caused by constant repetition of keystrokes: In a single shift, a word processor may perform 23,000 keystrokes. Symptoms of carpal tunnel syndrome include numbness, shooting pain, inability to grasp objects, and tingling. Millions of workers have been diagnosed with carpal tunnel syndrome.

RSI is avoidable. Designing workstations for a neutral wrist position (using a wrist rest to support the wrist), proper monitor stands, and footrests all contribute to proper posture and reduced RSI. New, ergonomically correct keyboards are also an option. These measures should be supported by frequent rest breaks and rotation of employees to different jobs.

RSI is not the only occupational illness computers cause. Back and neck pain, leg stress, and foot pain also result from poor ergonomic designs of workstations. **Computer vision syndrome (CVS)** refers to any eyestrain condition related to computer display screen use. Its symptoms, which are usually temporary, include headaches, blurred vision, and dry and irritated eyes.

The newest computer-related malady is **technostress**, which is stress induced by computer use. Its symptoms include aggravation, hostility toward humans, impatience, and fatigue. According to experts, humans working continuously with computers come to expect other humans and human institutions to behave like computers, providing instant responses, attentiveness, and an absence of emotion. Technostress is thought to be related to high levels of job turnover in the computer industry, high levels of early retirement from computer-intense occupations, and elevated levels of drug and alcohol abuse.

The incidence of technostress is not known but is thought to be in the millions and growing rapidly in the United States. Computer-related jobs now top the list of stressful occupations based on health statistics in several industrialized countries.

To date, the role of radiation from computer display screens in occupational disease has not been proved. Video display terminals (VDTs) emit nonionizing

electric and magnetic fields at low frequencies. These rays enter the body and have unknown effects on enzymes, molecules, chromosomes, and cell membranes. Long-term studies are investigating low-level electromagnetic fields and birth defects, stress, low birth weight, and other diseases. All manufacturers have reduced display screen emissions since the early 1980s, and European countries, such as Sweden, have adopted stiff radiation emission standards.

The computer has become a part of our lives—personally as well as socially, culturally, and politically. It is unlikely that the issues and our choices will become easier as information technology continues to transform our world. The growth of the Internet and the information economy suggests that all the ethical and social issues we have described will be heightened further as we move into the first digital century.

4.4 Hands-on MIS

The projects in this section give you hands-on experience in developing a privacy policy for a real-world company, using Web page development tools to design and create a simple Web site, and using Internet newsgroups for market research.

Developing a Web Site Privacy Policy

Software skills: Web browser software and presentation software
Business skills: Corporate privacy policy formulation

Dirt Bikes's management wants to make sure it has policies and procedures in place to protect the privacy of visitors to its Web site. You have been asked to develop Dirt Bikes's Web site privacy policy. The TRUSTe Web site at www.truste.org has Model Privacy Disclosures in its Privacy Resources that you can download and review to help you draft Dirt Bikes's privacy policy. You can also examine specific companies' privacy policies by searching for Web site privacy policies on Yahoo!, Google, or another search engine. Prepare a report for management that addresses the following issues:

- How much data should Dirt Bikes collect on visitors to its Web site? What information could it discover by tracking visitors' activities at its Web site? What value would this information provide the company? What are the privacy problems raised by collecting such data?
- Should Dirt Bike use cookies? What are the advantages of using cookies for both Dirt Bikes and its Web site visitors? What privacy issues do they create for Dirt Bikes?
- Should Dirt Bikes join an organization such as TRUSTe to certify that it has adopted approved privacy practices? Why or why not?
- Should Dirt Bikes design its site so that it conforms to P3P standards? Why or why not?
- Should Dirt Bikes adopt an opt-in or opt-out model of informed consent?
- Include in your report a short (two to three pages) privacy statement for the Dirt Bikes Web site. You can use the categories of the TRUSTe Model Privacy Disclosures as a guideline if you wish.
- (Optional) Use electronic presentation software to summarize your recommendations for management.

Achieving Operational Excellence: Creating a Simple Web Site Using Web Page Development Tools

Software skills: Web page creation
Business skills: Web page design

In this project, you will learn how to build a simple Web site of your own design for a business using the Web page creation function of Microsoft Word, Microsoft FrontPage, or a Web page development tool of your choice.

Build a simple Web site for a business. The Web site should include a home page with a description of your business and at least one picture or graphic. From the home page, you must be able to link to a second Web page and, from there, link to a third Web page. Make the home page long enough so that when you arrive at the bottom of the page, you can no longer see the top. At the bottom of your Web page include a link back to the top. Also include a link to one of the secondary Web pages. On the secondary page, include a link to the top of that page and a link back to the top of the homepage. Also include a link to the third page, which should contain a link to its own top and a link back to the top of the home page. Finally, on one of the secondary pages, include another picture or graphic, and on the other page include an object that you create using Microsoft Excel or other spreadsheet software. The Laudon Web site for Chapter 4 includes instructions for completing this project. If you have tested every function and all work to your satisfaction, save the pages you have created for submission to your instructor.

Improving Decision Making: Using Internet Newsgroups for Online Market Research

Software Skills: Web browser software and Internet newsgroups
Business Skills: Using Internet newsgroups to identify potential customers

This project will help develop your Internet skills in using newsgroups for marketing. It will also ask you to think about the ethical implications of using information in online discussion groups for business purposes.

You are producing hiking boots that you are selling through a few stores at this time. You think your boots are more comfortable than those of your competition. You believe you can undersell many of your competitors if you can significantly increase your production and sales. You would like to use Internet discussion groups interested in hiking, climbing, and camping both to sell your boots and to make them well known. Visit Google's Usenet archives (groups.google.com), which stores discussion postings from many thousands of newsgroups. Through this site you can locate all relevant newsgroups and search them by keyword, author's name, forum, date, and subject. Choose a message and examine it carefully, noting all the information you can obtain, including information about the author.

- How could you use these newsgroups to market your boots?
- What ethical principles might you be violating if you use these messages to sell your boots? Do you think there are ethical problems in using newsgroups this way? Explain your answer.
- Next use Google or Yahoo.com to search for the hiking boots industry and locate sites that will help you develop other new ideas for contacting potential customers.

- Given what you have learned in this and previous chapters, prepare a plan to use newsgroups and other alternative methods to begin attracting visitors to your site.

Learning Track Module

Developing a Corporate Code of Ethics for Information Systems. This Learning Track module describes the outline for a corporate code of ethics in information systems. What should be in a code of ethics? What ethical dimensions should be included? The Learning Track module is available at the Laudon Web site for this chapter and on the Student CD-ROM.

Summary

1. *Analyze the relationships among ethical, social, and political issues that are raised by information systems.*

Information technology has raised new possibilities for behavior for which laws and rules of acceptable conduct have not yet been developed. Information technology is introducing changes that create new ethical issues for societies to debate and resolve. Increasing computing power, storage, and networking capabilities—including the Internet—can expand the reach of individual and organizational actions and magnify their impacts. The ease and anonymity with which information can be communicated, copied, and manipulated in online environments are challenging traditional rules of right and wrong behavior. Ethical, social, and political issues are closely related. Ethical issues confront individuals who must choose a course of action, often in a situation in which two or more ethical principles are in conflict (a dilemma). Social issues spring from ethical issues as societies develop expectations in individuals about the correct course of action. Political issues spring from social conflict and are mainly concerned with using laws that prescribe behavior to create situations in which individuals behave correctly.

2. *Identify the main moral dimensions of an information society and specific principles for conduct that can be used to guide ethical decisions.*

The moral dimensions of information systems center around information rights and obligations, property rights and obligations, accountability and control, system quality, and quality of life. Six ethical principles are available to judge conduct. These principles are derived independently from several cultural, religious, and intellectual traditions and include the Golden Rule, Immanuel Kant's Categorical Imperative, Descartes' rule of change, the Utilitarian Principle, the Risk Aversion Principle, and the ethical "no free lunch" rule. These principles should be used in conjunction with an ethical analysis to guide decision making. The ethical analysis involves identifying the facts, values, stakeholders, options, and consequences of actions. Once completed, you can consider which ethical principle to apply to a situation to arrive at a judgment.

3. *Evaluate the impact of contemporary information systems and the Internet on the protection of individual privacy and intellectual property.*

Contemporary information systems technology, including Internet technology, challenges traditional regimens for protecting individual privacy and intellectual property. Data storage and data analysis technology enables companies to easily gather personal data about individuals from many different sources and analyze these data to create detailed electronic profiles about individuals and their behaviors. Data flowing over the Internet can be monitored at many points. The activities of Web site visitors can be closely tracked using cookies and other Web monitoring tools. Not all Web sites have strong privacy protection policies, and they do not always allow for informed consent regarding the use of personal information. The online industry prefers self-regulation to the U.S. government tightening privacy protection legislation.

Traditional copyright laws are insufficient to protect against software piracy because digital material can be copied so easily. Internet technology also makes intellectual property even more difficult to protect because digital material can be copied easily and transmitted to many different locations simultaneously over the Net. Web pages can be constructed easily using pieces of content from other Web sites without permission.

4. *Assess how information systems have affected everyday life.*

Although computer systems have been sources of efficiency and wealth, they have some negative impacts. Errors in large computer systems are impossible to eradicate totally. Computer errors can cause serious harm to individuals and organizations, and existing laws and social practices are often unable to establish liability and accountability for these problems. Less serious errors are often attributable to poor data quality, which can cause disruptions and losses for businesses. Jobs can be lost when computers replace workers or tasks become unnecessary in reengineered business processes. The ability to own and use a computer may be exacerbating socioeconomic disparities among different racial groups and social classes. Widespread use of computers increases opportunities for computer crime and computer abuse. Computers can also create health problems, such as repetitive stress injury, computer vision syndrome, and technostress.

Key Terms

Accountability, 135
Carpal tunnel syndrome (CTS), 155
Computer abuse, 152
Computer crime, 152
Computer vision syndrome (CVS), 156
Cookies, 142
Copyright, 145
Descartes' rule of change, 137
Digital divide, 155
Digital Millennium Copyright Act (DMCA), 147
Due process, 136
Ethical "no free lunch" rule, 137
Ethics, 128
Fair Information Practices (FIP), 140
Golden Rule, 137
Immanuel Kant's Categorical Imperative, 137
Information rights, 130
Informed consent, 141
Intellectual property, 145
Liability, 136
Nonobvious relationship awareness (NORA), 132
Opt-in, 143
Opt-out, 143
P3P, 144
Patent, 146
Privacy, 139
Profiling, 131
Repetitive stress injury (RSI), 155
Responsibility, 135
Risk Aversion Principle, 137
Safe harbor, 141
Spam, 152
Spyware, 142
Technostress, 156
Trade secret, 145
Utilitarian Principle, 137
Web bugs, 142

Review Questions

1. In what ways are ethical, social, and political issues connected? Give some examples.

2. What are the key technological trends that heighten ethical concerns?

3. What are the differences between responsibility, accountability, and liability?

4. What are the five steps in an ethical analysis?

5. Identify and describe six ethical principles.

6. What is a professional code of conduct?

7. What are meant by privacy and fair information practices?

8. How is the Internet challenging the protection of individual privacy?

9. What role can informed consent, legislation, industry self-regulation, and technology tools play in protecting the individual privacy of Internet users?

10. What are the three different regimes that protect intellectual property rights? What challenges to intellectual property rights does the Internet pose?

11. Why is it so difficult to hold software services liable for failure or injury?
12. What is the most common cause of system quality problems?
13. Name and describe four quality-of-life impacts of computers and information systems.
14. What is technostress, and how would you identify it?
15. Name three management actions that could reduce RSI injuries.

Discussion Questions

1. Should producers of software-based services, such as ATMs, be held liable for economic injuries suffered when their systems fail?
2. Should companies be responsible for unemployment caused by their information systems? Why or why not?

Video Case

You will find a video case illustrating some of the concepts in this chapter on the Laudon Web site and Student CD-ROM along with questions to help you analyze the case.

Teamwork: Developing a Corporate Ethics Code

With three or four of your classmates, develop a corporate ethics code on privacy that addresses both employee privacy and the privacy of customers and users of the corporate Web site. Be sure to consider e-mail privacy and employer monitoring of worksites, as well as corporate use of information about employees concerning their off-the-job behavior (e.g., lifestyle, marital arrangements, and so forth). If possible, use electronic presentation software to present your ethics code to the class.

Is the Telephone Company Violating Your Privacy?
CASE STUDY

In May 2006, *USA Today* reported that three of the four major United States landline telecommunications companies had cooperated with the National Security Agency (NSA) fight against terrorism by turning over records of billions of phone calls made by Americans. AT&T, Verizon Communications, and BellSouth all contributed to the NSA's anti-terrorism program. Qwest Communications International was the only one of the big four to withhold its records.

The revelation by *USA Today* caused a firestorm of controversy. Media outlets, privacy advocates, and critics of the Bush administration expressed outrage over the program and questioned its legality. The *Washington Post* referred to the program as a "massive intrusion on personal privacy."

The issue received particularly strong scrutiny because it came to light only five months after President Bush said that he had authorized the NSA to listen in on international phone calls of Americans suspected of having ties to terrorism without obtaining a warrant. When combined, the two stories caused intense worry among privacy activists who feared that a widespread data mining effort was being carried out against American citizens by the administration.

President Bush would not acknowledge the existence of such an initiative. He said only that, "the intelligence activities I authorized are lawful and have been briefed to appropriate members of Congress." He added, "We are not mining or trolling through the personal lives of innocent Americans" and the privacy of citizens was being "fiercely protected."

What exactly did the phone companies do for the government? After September 11, 2001, they began turning over tens of millions of phone call records to the NSA, whose goal was to build a database of every call made inside the United States. The records that were turned over contained only phone numbers and calling information such as time, date, and the duration of the calls; they omitted names, addresses, and other personal data. Qwest was approached by the NSA at the same time as the others, but Joseph Nacchio, the company's CEO at the time (later involved in an insider trading scandal), refused to cooperate. Nacchio based his decision on the fact that the NSA had not secured a warrant or submitted to other legal processes in requesting the data.

The ethical questions raised by this case prompted no shortage of opinions from executives, politicians, pundits, activists, and legal experts. The phone companies cited a strong belief in protecting the privacy of their customers but stated that the belief must co-exist with an obligation to cooperate with law enforcement and the government in matters of national security. A release from AT&T summed up the company's position as follows: "If and when AT&T is asked to help, we do so strictly within the law and under the most stringent conditions." Verizon made a similar statement but also declined to comment on having a connection to a "highly classified" national security plan. The company also indicated that press coverage of its data dealings contained factual errors.

After examining the issue, legal experts on both sides of it weighed in with their opinions on the actions taken by the phone companies. Lawmakers began to seek hearings on the matter almost immediately. Customers directed their anger and concern directly to customer support lines. Two lawyers in New Jersey filed a $5 billion suit against Verizon on behalf of the public accusing the company of violating privacy laws.

Some legal scholars and privacy advocates agree that the telecoms may have crossed the line. These experts cite the Electronic Privacy Act of 1986, which permits businesses to turn over calling data to the government only in extreme cases (for example, to protect individuals who are in immediate danger of being harmed). Creating a database from the records does not meet the criteria. James X. Dempsey of the Center for Democracy and Technology noted that the law allows for a minimum penalty of $1,000 per customer whose calling data were submitted to the government. Based on the number of records contributed to the NSA database, the phone companies faced civil penalties reaching hundreds of millions or possibly billions of dollars.

Dempsey shot down the idea that the phone companies did not break the law because the records they turned over included only phone numbers and

not identifying information. According to Dempsey, the law does not specify that such personal information needs to be exchanged for the law to be broken. This was a popular position among critics of the NSA program. They asserted that phone numbers could easily be cross-referenced to personal information, such as names and addresses, using databases that are readily available to the public on the Internet.

A senior government official who spoke on condition of anonymity admitted that the NSA had access to most domestic telephone calls even though, according to Kate Martin of the Center for National Security Studies, the NSA would be prohibited by federal statutes from obtaining such data without judicial consent. The government official said that the scope of the program was small in the sense that the database was used only to track the communications of individuals who were known to have ties to terrorism.

The non-profit Electronic Frontier Foundation (EFF), a privacy watchdog, concurs with Martin's assessment. EFF supports its argument by referencing the Pen Register Statute, which prohibits the government from gathering calling data without a court order, and the Fourth Amendment, which covers privacy rights and unreasonable search and seizure. However, the impact of such a defense in court was unclear. In response to the wiretapping controversy of five months earlier, the Bush administration cited Article II of the Constitution as the derivation of its authority to employ wiretapping as a terror-fighting tool. Furthermore, Congress virtually wrote the President a blank check by empowering him to "use all necessary and appropriate force" in the war on terror.

It was not surprising that Congress had as much to say about the issue as anyone. Various senators weighed in both with opinions and calls for investigation. Opinions did not always fall along party lines.

Senator Dick Durbin, a Democrat from Illinois, believed that actions of the telephone companies put the privacy of American citizens at stake and that the companies should be compelled to appear before the Senate Judiciary Committee. Durbin was backed up by the chairman of that committee, Senator Arlen Specter, a Republican from Pennsylvania. Senator Specter intended to call upon executives from the participating companies to give their testimony about the NSA database program. House Majority Leader John Boehner of Ohio and Senator Lindsey Graham of South Carolina also crossed party lines in questioning the necessity of such a program. Senator Graham asked, "The idea of collecting millions of thousands of phone numbers, how does that fit into following the enemy?"

Proponents of the program answer that question by saying that the purpose of the program is to discover patterns in the calling records that indicate the presence of terrorist activity. Intelligence analysts and commercial data miners refer to this as "link analysis," which is a technique for pulling meaningful patterns out of massive quantities of data. Defenders of the program were harshly critical of media outlets who exposed it. Representative Peter Hoekstra, a republican from Michigan and chairman of the House Intelligence Committee, insisted that reporting on the NSA's programs undermined national security. He stated, "Rather than allow our intelligence professionals to maintain a laser focus on the terrorists, we are once again mired in a debate about what our intelligence community may or may not be doing." President Bush echoed this sentiment by declaring that leaks of sensitive intelligence always hurt the government's ability to counter terrorism.

Republican Senator Jeff Sessions of Alabama also disputed the need to investigate the program. Senator Sessions answered the critics by emphasizing that the program did not involve actual surveillance of phone conversations and therefore did not merit the scrutiny it was receiving. In his statements, the president also went out of his way to distinguish between eavesdropping on telephone conversations and gathering call data.

In May 2006, senior intelligence officials revealed that the scope of the NSA's eavesdropping operations was strongly influenced by Vice President Dick Cheney and his office. The Vice President and his key legal adviser, David S. Addington, began pushing for surveillance of domestic phone calls and e-mails without warrants soon after September 11th. They believed that the Constitution gave the executive branch expansive powers that covered this type of domestic spying, as well as certain interrogation tactics for dealing with suspected terrorists. However, the NSA pushed back on advice from its own legal team. As a result, the NSA limited the eavesdropping to calls in which at least one participant was outside the United States.

Still, conducting such operations appeared to conflict with the 1978 Foreign Intelligence Surveillance Act (FISA), which required court authorization for any wiretapping done within the United States. Nancy Libin of the Center for Democracy and

Technology posits that listening in on any phone call without a warrant, regardless of whether it is domestic or international, is illegal according to FISA. However, while FISA covers wiretapping, it does not clearly prohibit the type of data mining was that done in the NSA database program.

In June 2006, a federal court in California released a document related to EFF's suit against AT&T that sheds light on how the phone company may have provided its data to the NSA. In the document, J. Scott Marcus, who had worked as a senior advisor for Internet technology to the Federal Communications Commission, evaluates evidence presented to EFF from a former AT&T technician named Mark Klein. Klein claimed that AT&T reconfigured its network in San Francisco and installed special computer systems in a secret room in order to divert and collect Internet traffic for use by the NSA. Marcus concluded that Klein's description of a private backbone network partitioned from AT&T's main Internet backbone was "not consistent with normal AT&T practice." Marcus further observed that at the time of the reconfiguration, AT&T was in poor shape financially and would have been very unlikely to have made such expensive infrastructure changes on its own.

In July 2006, Senator Specter announced that an agreement had been reached with the White House to give the Foreign Intelligence Surveillance Court the authority to review the constitutionality of the NSA's surveillance programs. The court would be empowered to determine whether wiretapping fell within the president's powers to fight the war on terrorism. The agreement allowed for the court's proceedings and rulings to be conducted in secret. Even though judicial oversight of the NSA's activities had been established, debate continued over the efficacy of the compromise. The American Civil Liberties Union and the ranking democrat on the House Intelligence Committee, Representative Jane Harman of California, accused Senator Specter of giving away too much, including a key Fourth Amendment protection.

The White House won several important points in the agreement, including the ability to appeal the court's decisions; changing the language so that submitting a program to the court was actually optional for the administration; and a guarantee that the agreement does not retract any of the president's existing constitutional authority. On the other hand, the lead judge on the court was known to have significant misgivings about the NSA's actions even before the program came to light. The bill to enact FISA's power over NSA wiretapping awaits Congressional approval.

Sources: Lauren Etter, "Is the Phone Company Violating Your Privacy?" *The Wall Street Journal*, May 13, 2006; Dionne Searcy, Amy Schatz, and Amol Sharma, "Phone Firms May Be On the Hook For Aiding U.S. Data-Mining Efforts," *The Wall Street Journal*, May 13, 2006; Eric Lichtblau and Scott Shane, "Bush Is Pressed Over New Report on Surveillance," *The New York Times*, May 11, 2006; "The Datamining Scare," *The Wall Street Journal*, May 13, 2006; Eric Lichtblau, "Bush Would Let Secret Court Sift Wiretap Process," *The New York Times*, July 14, 2006; Scott Shane and Eric Lichtblau, "Cheney Pushed U.S. to Widen Eavesdropping," *The New York Times*, May 14, 2006; "Deal Reached on Eavesdropping Program Oversight," CNN.com, July 13, 2006; John Markoff, "Questions Raised for Phone Giants in Spy Data Furor," *The New York Times*, May 13, 2006; Kim Zetter, "New Light on NSA Spying," Salon.com, June 23, 2006.

CASE STUDY QUESTIONS

1. Do the increased surveillance power and capability of the U.S. government present an ethical dilemma? Explain your answer.
2. Apply an ethical analysis to the issue of the U.S. government's use of telecommunications data to fight terrorism.
3. What are the ethical, social, and political issues raised by the U.S. government creating massive databases to collect the calling data of millions of Americans?
4. What is the responsibility of a business such as AT&T or Verizon in this matter? What are the ethical, social, and political issues raised by a business, such as a phone company, working with the government in this fashion?
5. State your opinion of the agreement reached by the White House and the Senate Judiciary Committee with regard to the NSA wiretapping program. Is this an effective solution?